9.1.1 ArgumentationElement class (abstract)

An ArgumentationElement is the top level element of the hierarchy for argumentation elements.

Attributes

- description: String
  A description of the Argumentation entity.
- content: String
  Supporting content of the Argumentation entity.

Semantics

The ArgumentationElement is a common class for all elements within a structured argument.

9.1.2 Argumentation Class

The Argumentation Class is the container class for a structured argument represented using the SACM Argumentation Metamodel.

Superclass

ModelElement

Associations

- argumentElement:ArgumentElement[0..*]
  The ArgumentElements contained in a given instance of an Argumentation.
- argumentation:Argumentation[0..*]
  The nested Argumentation contained in a given instance of an Argumentation.

Semantics

Structured arguments represented using the Argumentation Metamodel are composed of ArgumentElements. Argumentation elements can be nested.

For example, arguments can be established through the composition of Claims (propositions) and the AssertedInferences between those Claims.

Example

See Annex B.

~~<ARM:Argument xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ARM="ARM" xmi:id="0">~~
~~</ARM:Argument>~~

9.1.3 ArgumentElement Class (Abstract)

The ArgumentElement Class is the abstract class for the elements of any structured argument represented using the Argumentation Metamodel.

Superclass

ModelElement

Semantics

ArgumentElements represent the constituent building blocks of any structured Argument.

For example, ArgumentElements can represent the Claims made within a structured Argument.

9.1.4 Assertion Class (Abstract)

Assertions are used to record the propositions of Argumentation (including both the Claims about the subject of the argument and structure of the Argumentation being asserted). Propositions can be true or false, but cannot be true and false simultaneously.

Superclass

ReasoningElement

Semantics

Structured arguments are declared by stating claims, citing evidence and contextual information, and asserting how these elements relate to each other.

9.1.5 ReasoningElement Class (Abstract)

The ReasoningElement Class is the abstract class for the elements that comprise the core reasoning of any structured argument represented using the Argumentation Metamodel – Assertions and ArgumentReasoning (the description of inferential reasoning that exists between Claims.

Superclass

ArgumentElement

Semantics

The core of any argument is the reasoning that exists to connect assertions of that argument. Reasoning is captured in the SACM through the linking of fundamental claims and the description of the relationships between the claims. ReasoningElements represent these two elements.

9.1.6 InformationElement Class

The InformationElement Class enables the inclusion or citation of a source of information that *relates* to the structured argument.. The declaration of relationship is made by the AssertedRelationship class.

Superclass

ArgumentElement

Attributes

Associations

Example

See Annex B.

Semantics

It is necessary to be able to cite sources of information or directly provide information, that support, provide context for, or provide additional description for the core reasoning of the recorded argument. InformationElements allow there to be a provision of, objectified citation of this information within the structured argument, thereby allowing the relationship between this information and the argument to also be explicitly declared.

Example

See Annex B.

~~<containsArgumentElement xsi:type="ARM:Claim" xmi:id="5" identifier="C1.1" description="" content="Unintended opening of press (after PoNR) can only occur as a result of component failure"/>~~

~~9.1.9 EvidenceAssertion Class~~

~~A sub-type of Claim used to record propositions (assertions) made regarding an InformationElement being used as supporting evidence to the Argument. This is intended to be used as an interface element to external evidence. An evidence assertion is a minimal assertion (proposition) about an item of evidence, and there is no supporting argumentation being offered within the current structured argument.~~

~~Superclass~~

~~Claim~~

~~Semantics~~

~~Well supported arguments are those where evidence can be cited that is said to support the most fundamental claims of the argument. It is good practice that these fundamental claims of the argument state clearly the property that is said to exist in, be derived from, or be exhibited by the cited evidence. Where such claims are made these are said to be basic EvidenceAssertions.~~

~~Example~~

~~<containsArgumentElement xsi:type="ARM:EvidenceAssertion" xmi:id="12" identifier="C2.1.1" content="Failure 1 of PLC state machine includes BUTTON_IN remaining true"/>~~

9

9.1.~~10~~ ArgumentReasoning Class

ArgumentReasoning can be used to provide additional description or explanation of the asserted inference or challenge that connects one or more Claims (premises) to another Claim (conclusion). ArgumentReasoning elements are therefore related to AssertedInferences and AssertedChallenges. It is also possible that ArgumentReasoning elements can refer to other structured Arguments as a means of documenting the detail of the argument that establishes the asserted inferences.

Superclass

ReasoningElement

Associations

- describedAssertedRelationship:AssertedRelationship[0..*]
  Reference to the AssertedRelationship being described by the ArgumentReasoning.
- structure:Argument[0..1]
  Optional reference to another structured Argument to provide the detailed structure of the Argument being described by the ArgumentReasoning.

Semantics

The argument step that relates one or more Claims (premises) to another Claim (conclusion) may not always be obvious. In such cases ArgumentReasoning can be used to provide further description of the reasoning steps involved.

Example

See Annex B.

~~<containsArgumentElement xsi:type="ARM:ArgumentReasoning" xmi:id="2" identifier="RC1.1" content="Argument by omission of all identified software hazards" describes="5 6"/>~~

10

9.1.~~11~~ AssertedRelationship Class (Abstract)

The AssertedRelationship Class is the abstract class that enables the ArgumentElements of any structured argument to be linked together. The linking together of ArgumentElements allows a user to declare the relationship that they assert to hold between these elements.

Superclass

Assertion

Associations

- source:ArgumentElement[0..*]
  Reference to the ArgumentElement(s) that are the source (start-point) of the relationship.
- target:ArgumentElement[0..*]
  Reference to the ArgumentElement(s) that are the target (end-point) of the relationship.

Semantics

In the SACM, the structure of an argument is declared through the linking together of primitive ArgumentElements. For example, a sufficient inference can be asserted to exist between two claims ("Claim A implies Claim B") or sufficient evidence can be asserted to exist to support a claim ("Claim A is evidenced by Evidence B"). An inference asserted between two claims (A – the source – and B – the target) denotes that the truth of Claim A is said to infer the truth of Claim B.

Example

See Annex B.

11

9.1.~~12~~ AssertedInference Class

The AssertedInference association class records the inference that a user declares to exist between one or more Assertion (premises) and another Assertion (conclusion). It is important to note that such a declaration is itself an assertion on behalf of the user.

Superclass

AssertedRelationship

Semantics

The core structure of an argument is declared through the inferences that are asserted to exist between Assertions (e.g., Claims). For example, an AssertedInference can be said to exist between two claims ("Claim A implies Claim B"). An AssertedInference between two claims (A – the source – and B – the target) denotes that the truth of Claim A is said to infer the truth of Claim B.

Example

See Annex B.

~~<containsAssertedRelationship xsi:type="ARM:AssertedInference" xmi:id="16" identifier="C1.1.1" description="" target="5" source="1"/>~~

Invariants

```
context AssertedInference
inv SourceMustBeAssertion : self.source->forAll(s|s.oclIsTypeOf(Assertion))
inv TargetMustBeAssertion : self.target->forAll(t|t.oclIsTypeOf(Assertion))
```

12

9.1.~~13~~ AssertedEvidence Class

The AssertedEvidence association class records the declaration that one or more items of Evidence (cited by InformationItems) provides information that helps establish the truth of a Claim. It is important to note that such a declaration is itself an assertion on behalf of the user. The information (cited by an InformationItem) may provide evidence for more than one Claim.

Superclass

AssertedRelationship

Semantics

Where evidence (cited by InformationItems) exists that helps to establish the truth of a Claim in the argument, this relationship between the Claim and the evidence can be asserted by an AssertedEvidence association. An AssertedEvidence association between some information cited by an InformationElement and a Claim (A – the source evidence cited – and B – the target claim) denotes that the evidence cited by A is said to help establish the truth of Claim B.

Example

See Annex B.

~~<containsAssertedRelationship xsi:type="ARM:AssertedEvidence" xmi:id="22" identifier="S1.1" target="10" source="5 6"/>~~

Invariants

```
context AssertedEvidence
inv SourceMustBeInformationElement : self.source->forAll(s|s.oclIsTypeOf(InformationElement))
inv TargetMustBeClaimOrAssertedRelationship : self.target->forAll(t|t.oclIsTypeOf(Claim) or
t.oclIsTypeOf(AssertedRelationship))
```

13

9.1.~~14~~ AssertedChallenge Class

The AssertedChallenge association class records the *challenge* (i.e., counter-argument) that a user declares to exist between one or more Claims and another Claim. It is important to note that such a declaration is itself an assertion on behalf of the user.

Superclass

AssertedRelationship

Semantics

An AssertedChallenge by Claim A (source) to Claim B (target) denotes that the truth of Claim A challenges the truth of Claim B (i.e., Claim A leads towards the conclusion that Claim B is false).

Invariants

```
context AssertedChallenge
inv SourceMustBeClaim : self.source->forAll(s|s.oclIsTypeOf(Claim))
inv TargetMustBeClaimOrAssertedRelationship : self.target->forAll(t|t.oclIsTypeOf(Claim) or
t.oclIsTypeOf(AssertedRelationship))
```

14

9.1.~~15~~ AssertedCounterEvidence Class

AssertedCounterEvidence can be used to associate evidence (cited by InformationElements) to a Claim, where this evidence is being asserted to infer that the Claim is *false*. It is important to note that such a declaration is itself an assertion on behalf of the user.

Superclass

AssertedRelationship

Semantics

An AssertedCounterEvidence association between some evidence cited by an InformationNode and a Claim (A – the source evidence cited – and B – the target claim) denotes that the evidence cited by A is counter-evidence to the truth of Claim B (i.e., Evidence A suggests the conclusion that Claim B is false).

Invariants

```
context AssertedCounterEvidence
inv SourceMustBeInformationElement : self.source->forAll(s|s.oclIsTypeOf(InformationElement))
inv TargetMustBeClaimOrAssertedRelationship : self.target->forAll(t|t.oclIsTypeOf(Claim) or
t.oclIsTypeOf(AssertedRelationship))
```

15

9.1.~~16~~ AssertedContext Class

The AssertedContext association class declares that the information cited by an InformationElement provides a context for the interpretation and definition of a Claim or ArgumentReasoning element.

Superclass

AssertedRelationship

Semantics

Claim and ArgumentReasoning often need contextual information to be cited in order for the scope and definition of the reasoning to be easily interpreted. For example, a Claim can be said to be valid only in a defined context ("Claim A is asserted to be true only in a context as defined by the information cited by InformationItem B" or conversely "InformationItem B is the valid context for Claim A"). A declaration (AssertedContext) of context (InformationItem) for a ReasoningElement (A – the contextual InformationItem – and B – the ReasoningElement) denotes that A is asserted to be valid contextual information for B (i.e., A defines context where the reasoning presented by B holds true).

Example

See Annex B.

~~<containsAssertedRelationship xsi:type="ARM:AssertedContext" xmi:id="21" identifier="CIRC1.1" target="4" source="2"/>~~

Invariants

```
context AssertedContext
inv SourceMustBeInformationElement :self.source->forAll(s|s.oclIsTypeOf(InformationElement))
inv TargetMustBeReasoningElement : self.target->forAll(t|t.oclIsTypeOf(ReasoningElement))
```

16

9.1.~~17~~ InformationCitationElement Class

The InformationElementCitation Class enables the citation of a source of information that relates to the structured argument. The citation is made by the InformationElement class. The declaration of relationship is made by the AssertedRelationship class.

Superclass

InformationElement

Attributes

- url: String

An attribute recording a URL to external evidence.

Associations

- evidenceElement:Evidence::EvidenceElement[0..*]
  The EvidenceElements cited by the current InformationElementCitation object.
- evidenceContainer:Evidence::EvidenceContainer[0..*]
  The EvidenceContainer cited by the current InformationElementCitation object.
- assuranceCase:AssuranceCase[0..*]
  The assuranceCase cited by the current InformationElementCitation object.
- argumentation:Argumentation[0..*]
  The argumentation structure cited by the current InformationElementCitation object.

Semantics

It is necessary to be able to cite sources of information (EvidenceElements, EvidenceContainers, entire AssuranceCases, entire Argumentation structures, or external objects) that support, provide context for, or provide additional description for the core reasoning of the argumentation structure. InformationCitationElements allow there to be an objectified citation of this information within the argumentation structure, thereby allowing the relationship between this information and the argument to also be explicitly declared.

The url attribute is to be used when citing sources of information outside of an SACM model. The evidenceElement and evidenceContainer associations can only be used when conforming to the Assurance Case compliance point."

17

9.1.~~18~~ InformationProvisionElement Class

The InformationProvisionElement Class enables the direct provision of information that relates to the structured argument. The declaration of relationship is made by the AssertedRelationship class.

Superclass

InformationElement

Attributes

Associations

Semantics

It is sometimes necessary to directly provide sources of information, that support, provide context for, or provides additional description for the core reasoning of the recorded argument. InformationProvisionElements allow the provision of this information within the structured argument, thereby allowing the relationship between this information and the argument to also be explicitly declared.

EAssertion

FormalAssertion is an element of meaning that represents a certain proposition. The ~~Assertion~~ subclass, introduced in Clause 12 “Formal Statements” uses elements of formal statements and a formal reference to an SBVR vocabulary to represent precise meaning of the assertion. ReferencedClaim element represents an informal assertion/claim. Further details are provided in section 12 Formal Statements.

10.1.9 EvidenceGroup

EvidenceGroup asserts a state of affairs that several evidence elements are grouped together and can be referred to collectively.

Superclass

EvidenceItem

Attributes

- name:String
  Name of the evidence group.

Associations

- element:EvidenceElement[0..*1]
  Elements of the Evidence Group

Constraints

- EvidenceGroup can not be an element of itself, either directly or indirectly through membership in other Evidence Group.

Semantics

EvidenceGroup asserts a state of affairs that several evidence elements are grouped together and can be referred to collectively. EvidenceGroup is a special subclass of EvidenceItem acting as a named container for evidence items that can be used on both sides of an evidence relation. An EvidenceElement may be a member of more than one EvidenceGroup.

12 Formal Statements

12.1 General

Formal Statements provide the mechanism for representing the elements of meaning involved in the processes of interpretation and evaluation of evidence, and specifically, required for precisely representing assertions and claims.

The two fundamental classes of the Formal Statements are FormalObject and FormalAssertion. A FormalObject is an object of significance, about which information needs to be known or held. Usually a FormalObject corresponds to an Exhibit where the Exhibit element emphasizes the physical object (an instance of the SBVR 'Thing' concept) while a FormalObject emphasizes the associated element of meaning (an instance of the SBVR 'Meaning' concept). A FormalAssertion is a relationship between evidence elements taken as a new assertion/claim that has a distinct, separate existence, a self-contained piece of information that can be referenced as a unit. In the scope of SBVR, such units of information are called facts. However, since the Evidence Metamodel focuses at describing evidentiary support to assurance cases, which involves contestable claims, relationships are interpreted as assertions, rather than facts, which allows contesting them. However, in practice, most of the assertions that may be represented by an evidence model are likely to be within the so-called assumption zone of an assurance case, i.e., be agreed upon facts.

So, a FormalAssertion element represents an assertion involving one or more FormalObjects bound to specific roles associated with the fact type of the assertion. The concepts fact type, role, element is bound to a role are defined in SBVR. In particular, a fact type is defined as a concept that is the meaning of a verb phrase that involves one or more noun concepts and whose instances are all actualities. A role is defined as a noun concept that corresponds to things based on their playing a part, assuming a function, or being used in some situation. Specifically, a fact type role characterizes its instances by their involvement in an actuality that is an instance of a given fact type. A RoleBinding element represents an association, linkage, or connection between the FormalObjects that describes their role within the assertion.

Formal Statements are based on some pre-defined conceptual model related to the area for which an assurance case is developed. Such conceptual model can be formally represented as an external ontology or vocabulary. In particular the SACM Evidence Metamodel allows linking an Object element to an SBVR IndividualConcept or SBVR noun concept element and the ~~Assertion~~ element to SBVR fact type element.

EAssertion

The Object element is aligned with the SBVR IndividualConcept or the SBVR noun concept while the Assertion element is aligned with the SBVR fact type. Further, the entire SACM Evidence Metamodel is aligned with the OMG SBVR specification, in such a way that it describes a standard vocabulary related to descriptions of evidence. SBVR rules can be written using this vocabulary to formally describe further properties of evidence. The full SBVR vocabulary for evidence is presented as a non-normative Annex A.

12.2 Formal Objects Class Diagram

The FormalObjects class diagram focuses on objects that are involved in assertions comprising the fact model underlying an assurance case.

Semantics

From the formal logic perspective, SACM distinguishes objects from assertions. As a consequence, in order to represent a formal assertion about other assertions the later must be objectified, i.e., represented as a FormalObject that refers to the objectification of the original assertion using the element ObjectifiedAssertion.

12.3 Formal Assertions Class Diagram

The FormalAssertions class diagram focuses at the ~~Assertion~~ as the key element of the formal statements underlying an assurance case.

EAssertion

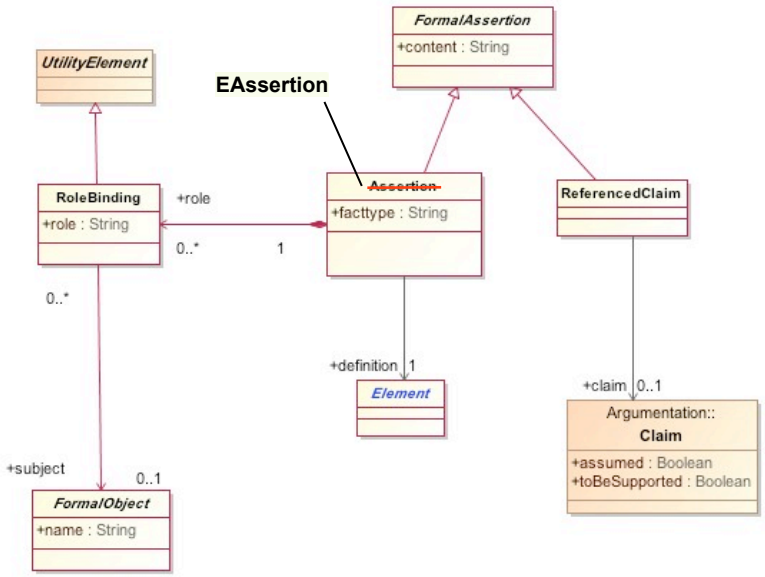


Figure 12.2 - Formal Assertions Class Diagram

12.3.1 ~~Assertion~~ —— EAssertion

EAssertion

An ~~Assertion~~ is a relationship involving one or more formal objects, taken as formal proposition that has a distinct, separate existence, a self-contained piece of information that can be referenced as a unit. ~~Assertion~~ is the key constituent of a conceptual model underlying an assurance case. ~~Assertion~~ represents an asserted fact about the subject area for which an assurance case is being developed.

EAssertion

Superclass

FormalAssertion

Attributes

- facttype:String
  Designation of the fact type.

Associations

- role:RoleBinding[0..*]
  Set of role bindings that further describe which FormalObjects are bound to the roles that are determined by the fact type.
- definition:MOF::Element
  A link to an entry of an external SBVR vocabulary or an OWL ontology defining the fact type of the assertion.

Semantics

EAssertion

~~Assertion~~ is an element of meaning that states existence of a relationship between several individual formal objects. In a formal assurance case, the nature of the relationship is specified through a reference to an external vocabulary, such as an SBVR vocabulary or an OWL ontology. SACM assumes that community of interest for an assurance case will acquire or develop such vocabularies for the corresponding subject area. In a semi-formal assurance case the nature of the relationship can be described informally through a 'content' property. In this case the 'definition' property and the 'facttype' property shall not be used. However the references to the exact FormalObjects through RoleBinding elements still can be stated. The 'content' property of the FormalAssertion element provides the verbalization of the assertion, which is the expression of the assertion in the selected natural language. For informal assurance cases, a ReferencedClaim element can be used, which only contains the verbalization of the claim in a natural language.

12.3.2 ReferencedClaim

ReferencedClaim is an element of meaning that represents an informal assertion about the state of affairs in the subject area about which an assurance case is developed. ReferencedClaim can be linked to a Claim element of the Argumentation part of an assurance case.

Superclass

FormalAssertion

Associations

- claim:Argumentation::Claim[0..1]
  A link to a Claim element in the Argumentation part of an assurance case (if available).

Semantics

ReferencedClaim is an element of meaning that makes an assertion about a subject area of an assurance case. ReferencedClaim represents the claim as prose in a selected natural language (formal or informal), without identifying its structure. ReferencedClaim element can represent informal claims (claims not linked to any formal definition of its meaning, such as an ontology developed by some community of meaning) or unstructured claims (where the subjects are not identified).

Usually claims assert existence of a formally defined relationship between several individual subjects and involve several objects bound to specific roles. An Assertion element can be used to capture this structure of a claim in a more formal way. In particular, Assertion element can link the proposition to an external vocabulary or ontology that defines the exact meaning of the proposition, as well as the exact subjects of the proposition.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<SACM:AssuranceCase xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ARM="http://schema.omg.org/SACM/1.0/Argumentation"
xmlns:EM="http://schema.omg.org/SACM/1.0/Evidence" xmlns:SACM="http://schema.omg.org/SACM/1.0" name="DoDAF
Analytics" gid="org.omg.sacm.examples-ac01-30072014">
  <argument>
```

EAssertion

RoleBinding instance is owned by an ~~Assertion~~ object that provides the context, including the definitions of roles and the types of domain objects that can be bound to each role. The formal definition of the relationship represented by an ~~Assertion~~ element is provided by a reference to an external ontology, which can be either an SBVR vocabulary or an OWL ontology. This definition shall at a minimum include the definition of roles, to which the RoleBinding elements shall conform. In particular, the 'role' attribute of a RoleBinding shall correspond to a particular role in the formal definition of a relationship. Further, for each role contained in the formal definition of the relationship there shall be exactly one RoleBinding element, in which the 'role' attribute matches the name of the role and the subject matches the allowed type of subject for that role.

SACM allows incremental construction of the conceptual model underlying an assurance case, therefore it allows temporarily unbound roles. A completed Body of Evidence accompanying an Assurance Case shall meet the condition that all RoleBinding elements have the corresponding subject of appropriate type.

SACM provides a built-in relation "IsA" between any EvidenceElement and an Object, which asserts the definition of an EvidenceItem. This mechanism can be used to build the entire formal vocabulary inside the Evidence Model, where the external references can be reduced to a mere handful of meta-meta level concepts (in the extreme case, the only external reference that is needed is the concept "thing," other definitions can, at least in principle, be provided through the "IsA" relationships internal to the Evidence Model. This approach can be used when the external formal vocabulary is not available, and there is a need to use more unified tooling environment.

From the formal logic perspective, SACM distinguishes objects from assertions. As a consequence, in order to represent a formal assertion about other assertions the later must be objectified, i.e., represented as a FormalObject that refers to the original assertion using the element ObjectifiedAssertion.

circumstantial evidence as it is often called) requires introduction of other pieces of information to complete a statement. Direct evidence has more weight than indirect. Whenever additional records are drawn to supply missing information there is a chance for error. Because of that, less weight is assigned to indirect evidence.

Support statement is verbalized as follows:

- "EvidenceItem directly supports FormalAssertion."
- "EvidenceItem indirectly supports FormalAssertion."
- "EvidenceItem directly challenges FormalAssertion."
- "EvidenceItem indirectly challenges FormalAssertion."

14.3.2 SupportLevel (enumeration)

SupportLevel enumeration specifies the support level.

Literals

- unknown
  The directness is unknown.
- indirect
  Evidence relation provides indirect support the ~~Assertion~~.
- direct
  Evidence relation provides direct support the ~~Assertion~~.

EAssertion

14.3.3 Reporting

Reporting statement represents a characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the reporting level of the relationship - primary or secondary reporting - provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:ReportingLevel
  Reporting level of the evidence relation, such as secondary or primary.

Constraints

- Reporting element shall not be owned by elements other than EvidenceRelation.

Semantics

Reporting level is an asserted characteristic that potentially can be disputed. Reporting level refers to the quality of information provided as evidence. For example, the record is primary if it was made at or near the time of the event, by someone in a position to know firsthand (such as an eyewitness). Alternatively, a record is considered primary if it was made in writing by an officer charged by law, canon, or bylaws with creating an accurate record. Primary information carries more weight than secondary

EAssertion

~~Assertion~~

Definition:	A proposition that is related to the area for which an assurance case is developed.
Description:	A formal assertion is a proposition that describes a state of affairs for which an assurance case is developed. This proposition uses the vocabulary that is imported from the semantic community involved in the subject area within which the evidence is collected. Formal assertions for evidence collection represent the asserted facts as part of the fact model corresponding to the body of evidence. Fact model is an SBVR term.
American Heritage Dictionary	Something declared or stated positively, often with no support or attempt at proof.
Note:	The term 'fact' is avoided because of the connotation with 'real' occurrences. Formal assertions can represent contradicting or conflicting propositions. The goal of the evidence-related effort is to establish the truth of certain propositions. During the course of the evidence collection and analysis project, various assertions may be considered.
Note:	Formal assertion is an instance of a fact type, a proposition that is formalized as an atomic formulation that binds to individual things.
Source:	**based on** Semantics of Business Vocabularies and Rules ['Fact']
Concept type:	meaning

Assertion *involves* Domain Object *in role* Subject Role

Definition:	
Concept type:	Facttype

Subject Role

Definition:	
Concept type:	Concept

A.5 Evidence Evaluation

A.5.1 Evidence Relations

Evidence Item *supports* Subject Assertion

Definition:	state of affairs **that** evidence item *supports* formal assertion.
Concept type:	state of affairs

Evidence Item *challenges* Subject Assertion

Definition:	an evidence judgment that an evidence item contradicts a formal assertion.
Concept type:	Evidence judgment

The Annex provides an example argument from the safety domain – a structured argument fragment for an industrial press.

In addition, details of the mappings from widely used existing notations – Goal Structuring Notation (GSN) and Claims, Arguments, Evidence (CAE) – which informed the development of SACM are also provided. Content written using these existing notations can therefore be exported using the elements of SACM for the purposes of data exchange.

Annex B - Examples

(non-normative)

B.1 General

~~The Annex provides two examples of argument from the safety and the security domain. The safety argument refers to an industrial press, whereas the security example is a fragment from a Bluetooth security case.~~

A

B.2 Industrial Press Safety Argument

~~<?xml version="1.0" encoding="ASCII"?>~~

~~<ARM:Argumentation xmi:version="2.1"~~

~~xmlns:xmi="http://schema.omg.org/spec/XMI/2.1"~~

~~xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"~~

~~xmlns:ARM="www.omg.org/spec/SACM/20120501/Argumentation"~~

~~xmi:id="0" id="IPSA">~~

~~<xsd:import namespace=http://schema.omg.org/spec/XMI/2.1" schemaLocation="http://www.omg.org/spec/XMI/20071213/XMI.xsd"/>~~

~~<xsd:import namespace="www.omg.org/spec/SACM/20120501/Argumentation" schemaLocation=" http://www.omg.org/spec/SACM/20120501/Argumentation.xsd" />~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="1" id="C1" description="" content="C/S logic is fault free"/>~~

~~<argumentElement xsi:type="ARM:ArgumentReasoning" xmi:id="2" id="RC1.1" content="Argument by omission of all identified software hazards" describes="5 6"/>~~

~~<argumentElement xsi:type="ARM:ArgumentReasoning" xmi:id="3" id="RC1.2" content="Argument by satisfaction of all C/S safety requirements" describes="7 8 9"/>~~

~~<argumentElement xsi:type="ARM:InformationElement" xmi:id="4" id="IRC1.1" description="Identified software hazards"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="5" id="C1.1" description="" content="Unintended opening of press (after PoNR) can only occur as a result of component failure"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="6" id="C1.2" description="" content="Unintended closing of press can only occur as a result of component failure"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="7" id="C2.1" content="Press controls being 'jammed on' will cause press to halt"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="8" id="C2.2" content="Release of controls prior to press passing physical PoNR will cause press operation to abort"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="9" id="C2.3" description="" content="C/S fails safe (halts on) and annunciates (by sounding Klaxon) all component failures" toBeSupported="true"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="12" id="C2.1.1" content="Failure 1 of PLC state machine includes BUTTON_IN remaining true"/>~~

~~<argumentElement xsi:type="ARM:Claim" xmi:id="13" id="C2.2.1" content="Abort transition of PLC state machine includes BUTTON_IN going false"/>~~

~~<argumentElement xsi:type="ARM:InformationElement" xmi:id="10" id="“S1.1" content="Fault tree analysis cutsets for event 'Hand trapped in press due to command error'"/>~~

~~<argumentElement xsi:type="ARM:InformationElement" xmi:id="11" id="“S1.2" content="Hazard directed test results"/>~~

~~<argumentElement xsi:type="ARM:InformationElement" xmi:id="14" id="“S2.1" description="" content="black box testing"/>~~

~~<argumentElement xsi:type="ARM:InformationElement" xmi:id="15" id="“S2.2.1" content="C/S state machine"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="16" id="“C1.1.1" description="" source="5" target="1"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="17" id="“C1.1.2" source="6" target="1"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="18" id="“C1.2.1" source="7" target="1"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="19" id="“C1.2.2" source="8" target="1"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="20" id="“C1.2.3" source="9" target="1"/>~~

~~<argumentElement xsi:type="ARM:AssertedContext" xmi:id="21" id="“CIRC1.1" source="4" target="2"/>~~

~~<argumentElement xsi:type="ARM:AssertedEvidence" xmi:id="22" id="“S1.1" source="10" target="5 6"/>~~

~~<argumentElement xsi:type="ARM:AssertedEvidence" xmi:id="23" id="“S1.2" source="11" target="5 6"/>~~

~~<argumentElement xsi:type="ARM:AssertedEvidence" xmi:id="24" id="“SC2.1" source="14" target="7"/>~~

~~<argumentElement xsi:type="ARM:AssertedEvidence" xmi:id="25" id="“SC2.1.1" source="15" target="12"/>~~

~~<argumentElement xsi:type="ARM:AssertedEvidence" xmi:id="26" id="“SC2.2.1" source="15" target="13"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="27" id="“DI C2.1" source="12" target="7"/>~~

~~<argumentElement xsi:type="ARM:AssertedInference" xmi:id="28" id="“DI C2.2" source="13" target="8"/>~~

~~<argumentElement xsi:type="ARM:AssertedContext" xmi:id="29" id="“AR29" source="2" target="16 17"/>~~

~~</ARM:Argumentation>~~

B.3 Bluetooth Security Case

<?xml version="1.0" encoding="ASCII"?>

<ARM:Argumentation xmi:version="2.1"

xmlns:xmi="http://schema.omg.org/spec/XMI/2.1"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:ARM=" www.omg.org/spec/SACM/20120501/Argumentation"

xmi:id="0" id="BSC11">

<xsd:import namespace=http://schema.omg.org/spec/XMI/2.1" schemaLocation="http://www.omg.org/spec/XMI/20071213/XMI.xsd"/>

<xsd:import namespace="www.omg.org/spec/SACM/20120501/Argumentation" schemaLocation=" http://www.omg.org/spec/SACM/20120501/Argumentation.xsd" />

<argumentElement xsi:type="ARM:Claim" xmi:id="1" id="“Bluetooth secure" content="A bluetooth enabled network provides adequate security"/ >

A


```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
Content generated by ASCE SACM Plugin version 0.1.5
 exported from W:\desktop\sacm\industrial press sketch_v01b.axml
 ASCE is available from http://www.adelard.com
-->
<ARM:Argumentation
        xmi:version="2.0"
        xmlns:xmi="http://www.omg.org/XMI"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ARM="http://schema.omg.org/SACM/1.1/Argumentation" >

<!-- ASCE nodes -->
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N1026380"
    id="N1026380"
    content="Release of controls prior to press passing physical PoNR will cause press operation to abort" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N1427811"
    id="N1427811"
    content="'Failure1' transition of PLC state machine includes BUTTON_IN remaining true" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N14509225"
    id="N14509225"
    content="'Abort' transition of PLC state machine includes BUTTON_IN going FALSE" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N25476474"
    id="N25476474"
    content="Unintended opening of press (after PoNR0 can only occur as a result of component failure" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N33411080"
    id="N33411080"
    content="C/S Logic is fault free" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:InformationElement"
    xmi:id="N46332973"
    id="N46332973"
    content="Black Box Test results" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:InformationElement"
    xmi:id="N50800675"
    id="N50800675"
    content="Identified software hazards" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:ArgumentReasoning"
    xmi:id="N5549157"
    id="N5549157"
    content="Argument by omission of all identified software hazards" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:ArgumentReasoning"
    xmi:id="N60452700"
    id="N60452700"
    content="Argument by satisfaction of all C/S safety requirements" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:InformationElement"
    xmi:id="N60541081"
    id="N60541081"
    content="C/S State Machine" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:Claim"
    xmi:id="N60938442"
    id="N60938442"
    content="Unintended closing of press can only occur as a result of component failure" >
</argumentElement>
  <argumentElement
    xsi:type="ARM:InformationElement"
    xmi:id="N74567521"
    id="N74567521"
    content="Hazard directed test results" >
```

A continued


```
</argumentElement>
  <argumentElement
      xsi:type="ARM:Claim"
      xmi:id="N75832051"
      id="N75832051"
      content="C/S fails safe (halts) on, and annunciates (by sounding klaxon), all single component failures” >
</argumentElement>
  <argumentElement
      xsi:type="ARM:InformationElement"
      xmi:id="N78302479"
      id="N78302479"
      content="Fault tree analysis cutsets for event 'Hand trapped in press due to command error’”>
</argumentElement>
  <argumentElement
      xsi:type="ARM:Claim"
      xmi:id="N91054195"
      id="N91054195"
      content="Press controlls being 'jammed on' will cause press to halt” >
</argumentElement>

<!-- ASCE links -->
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN1026380N60452700"
      source="N1026380"       target="N60452700" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN1427811N91054195"
      source="N1427811"       target="N91054195" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN14509225N1026380"
      source="N14509225"       target="N1026380" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN25476474N5549157"
      source="N25476474"       target="N5549157" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN46332973N91054195"
      source="N46332973"       target="N91054195" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedContext"
      xmi:id="LN50800675N5549157"
      source="N50800675"       target="N5549157" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN5549157N33411080"
      source="N5549157"       target="N33411080" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN60452700N33411080"
      source="N60452700"       target="N33411080" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN60541081N1427811"
      source="N60541081"       target="N1427811" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN60541081N14509225"
      source="N60541081"       target="N14509225" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN60938442N5549157"
      source="N60938442"       target="N5549157" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN74567521N25476474"
      source="N74567521"       target="N25476474" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN74567521N60938442"
      source="N74567521"       target="N60938442" >
```

A concluded


```
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN75832051N60452700"
      source="N75832051"       target="N60452700" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN78302479N25476474"
      source="N78302479"       target="N25476474" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedEvidence"
      xmi:id="LN78302479N60938442"
      source="N78302479"       target="N60938442" >
</argumentElement>
  <argumentElement
      xsi:type="ARM:AssertedInference"
      xmi:id="LN91054195N60452700"
      source="N91054195"       target="N60452700" >
</argumentElement>

</ARM:Argumentation>
```

```
<argumentElement xsi:type="ARM:InformationElement" xmi:id="10" id="“S1.1" content="Fault tree analysis cutsets for event 'Hand trapped in press due to command error'"/>

<argumentElement xsi:type="ARM:InformationElement"  xmi:id="11" id="“S1.2" content="Hazard directed test results"/>

<argumentElement xsi:type="ARM:InformationElement" xmi:id="14" id="“S2.1" description="" content="black box testing"/>

<argumentElement xsi:type="ARM:InformationElement"  xmi:id="15" id="“S2.2.1" content="C/S state machine"/>


<argumentElement xsi:type="ARM:AssertedInference" xmi:id="16" id="“C1.1.1" description="" source="5" target="1"/>

<argumentElement xsi:type="ARM:AssertedInference"  xmi:id="17" id="“C1.1.2" source="6" target="1"/>

<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
<argumentEl
</ARM:Argu
```


B.3 Mappings from existing industrial notations for assurance cases

B.3.1 Goal Structuring Notation (GSN)

Details of the mapping between GSN elements and SACM, and the available relevant tool support, are maintained at the following URL:

http://www.goalstructuringnotation.info/?p=291

B.3.2 Claims, Arguments, Evidence (CAE)

Details of the mapping between CAE elements and SACM, and the available relevant tool support, are maintained at the following URL:

http://www.adelard.com/asce/choosing-asce/standardisation.html

~~B.3 Bluetooth Security Case~~


```
<?xml version="1.0" encoding="ASCII"?>

<ARM:Argumentation xmi:version="2.1"

xmlns:xmi="http://schema.omg.org/spec/XMI/2.1"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:ARM=" www.omg.org/spec/SACM/20120501/Argumentation"

xmi:id="0" id="BSC11">

<xsd:import namespace=http://schema.omg.org/spec/XMI/2.1" schemaLocation="http://www.omg.org/spec/XMI/20071213/XMI.xsd"/>

<xsd:import namespace="www.omg.org/spec/SACM/20120501/Argumentation" schemaLocation=" http://www.omg.org/spec/SACM/20120501/Argumentation.xsd"/>

<argumentElement xsi:type="ARM:Claim" xmi:id="1" id="“Bluetooth secure" content="A bluetooth enabled network provides adequate security"/
>
```

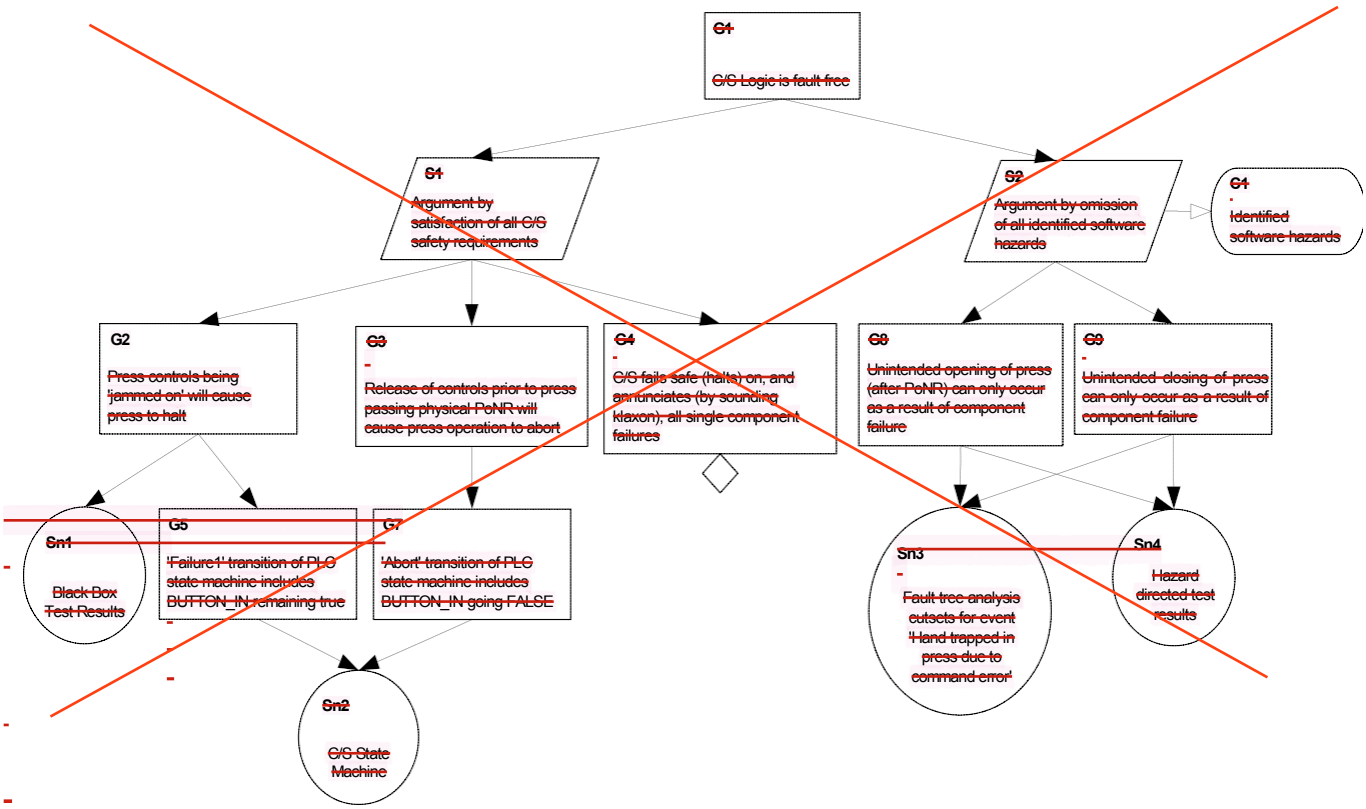
```
<argumentElement xsi:type="ARM: Claim" xmi:id="2" id="Availability" content="A bluetooth enabled network is adequately available [1] Section 1 para 3"/>

<argumentElement xsi:type="ARM: Claim" xmi:id="3" id="Access" description="" content="A bluetooth enabled network provides adequate control for access to services and data [1] Section 1 para 3"/>

<argumentElement xsi:type="ARM: Claim" xmi:id="4" id="Confidentiality" content="A bluetooth enabled network provides adequate levels of confidentiality [1] Setion 1 para 3"/>

<argumentElement xsi:type="ARM: Claim" xmi:id="5" id="Integrity" content="A bluetooth enabled network provides adequate levels of integrity [1] Section 1 para 3"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="6" id="Context: security policy and scenario for use" content="Definitions are required of the intented security policy and the scenario of use for the system, including what is regarded as 'adequate'"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="7" id="References" content="[1] Bluetooth security white paper 19/4/ 02"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="8" id="Definition: Availability" content="The system is capable of providing requested services to authorised users, in an acceptable/defined time"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="9" id="Definition: Access" content="Only users permitted by the defined security policy have access to services and data"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="10" id="Define: Confidentiality" content="Unauthorised persons cannot intercept and understand information to which they are not entitled"/>

<argumentElement xsi:type="ARM: InformationElement" xmi:id="11" id="Define: Integrity" description="" content="Services and data are provided to authorised users as intended and without corruption"/>


<argumentElement xsi:type="ARM: AssertedContext" xmi:id="12" id="AC1" source="7" target="1"/>

<argumentElement xsi:type="ARM: AssertedContext" xmi:id="13" id="AC2" source="6" target="1"/>

<argumentElement xsi:type="ARM: AssertedContext" xmi:id="14" id="AC3" source="8" target="2"/>

<argumentElement xsi:type="ARM: AssertedContext" xmi:id="15" id="AC4" source="9 " target="3"/>

<argumentElement xsi:type="ARM: AssertedContext" xmi:id="16" id="AC5" source="10" target="4"/>

<argumentElement xsi:type="ARM: AssertedContext" xmi:id="17" id="AC6" source="11" target="5"/>

<argumentElement xsi:type="ARM: AssertedInference" xmi:id="18" id="AI1" source="5 4 3 2" target="1"/>

<argumentElement xsi:type="ARM: ArgumentReasoning" xmi"id="19" id="Argue over vulnerabilities" description="" content="Argue for each security requirement identified in the security white paper" describes="18"/>

</ARM:Argument>
```

B.3.1 Goal Structuring Notation (GSN) Examples

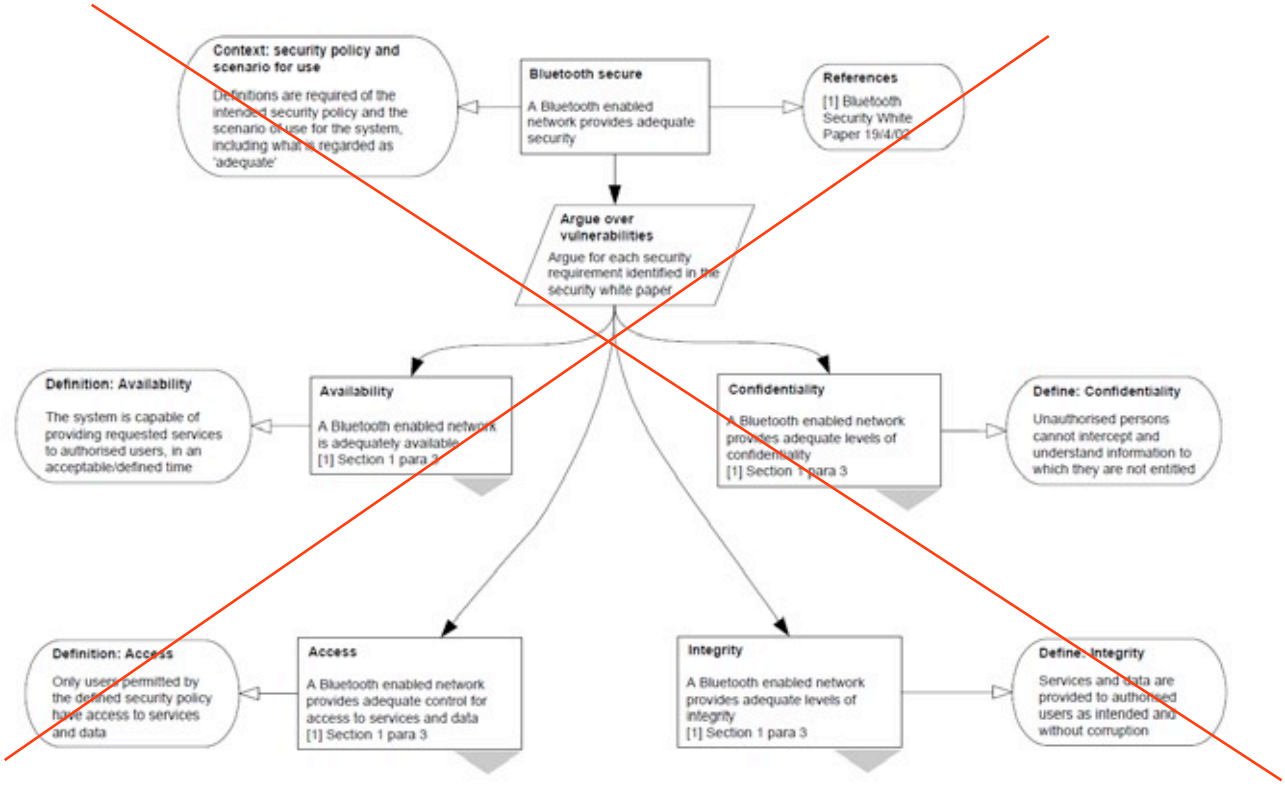
This section contains examples of arguments using the Goal Structuring Notation. The following table explains the relationship from the example to the modeling elements of SACM Argumentation Metamodel.

GSN element	SACM Argumentation Metamodel counterpart
Rectangle	Claim
Rounded rectangle	InformationElement

~~Parallelogram~~	~~ArgumentReasoning~~
~~Circle~~	~~InformationElement linked using an AssertedEvidence instance~~
~~Filled arrow~~	~~AssertedInference (or AssertedEvidence when linked to circle). The arrow head attaches to the source element.~~
~~Empty arrow~~	~~AssertedContext. The arrow head attaches to the source element.~~
~~Diamond decorator~~	~~ToBeSupported = true~~
~~Shaded triangle decorator~~	~~The current element is a citation element.~~



~~**Figure B.1 - Industrial Press Safety argument (§8.3.1)**~~



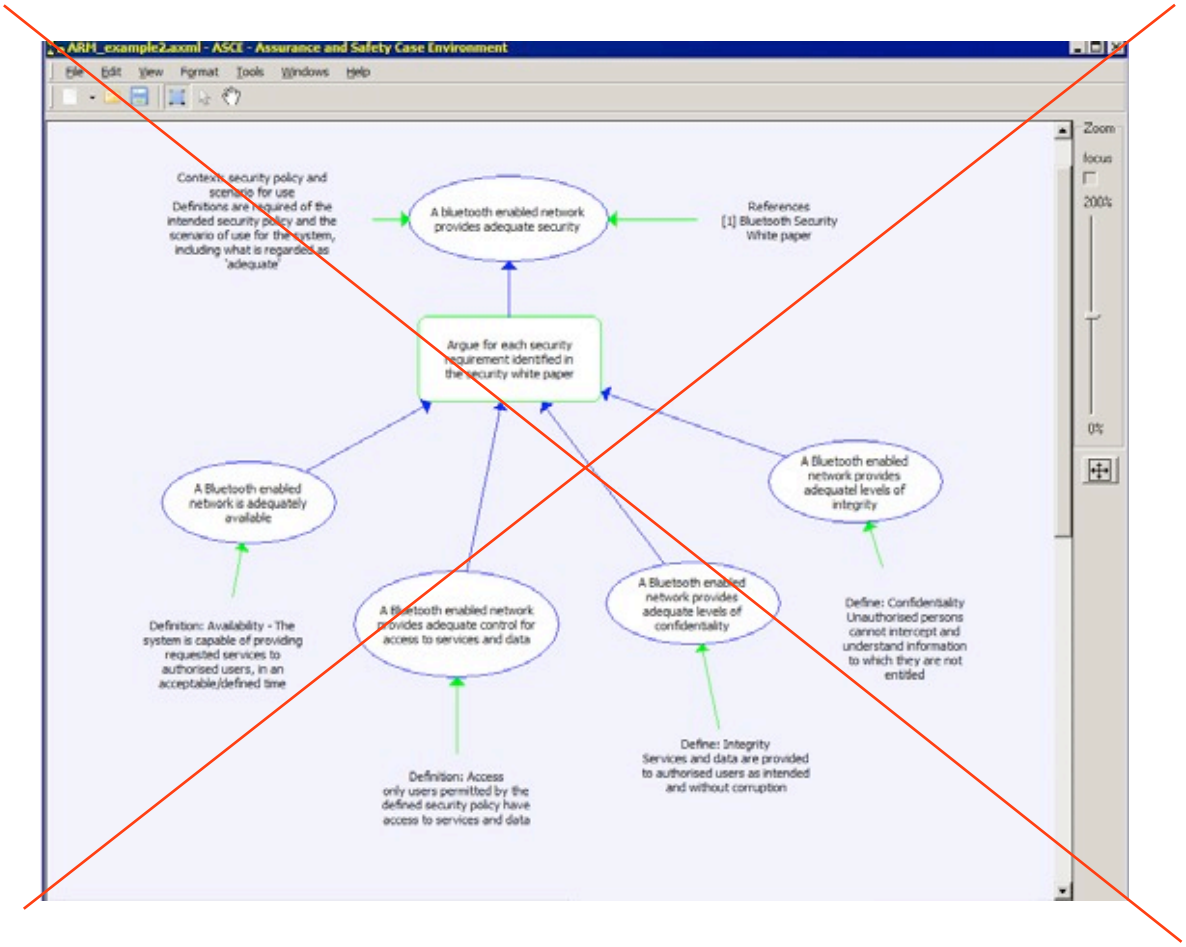
~~**Figure B.2 - GSN Bluetooth Security Case (§8.3.2)**~~

~~B.3.2 Claims-Arguments-Evidence (CAE) Example~~

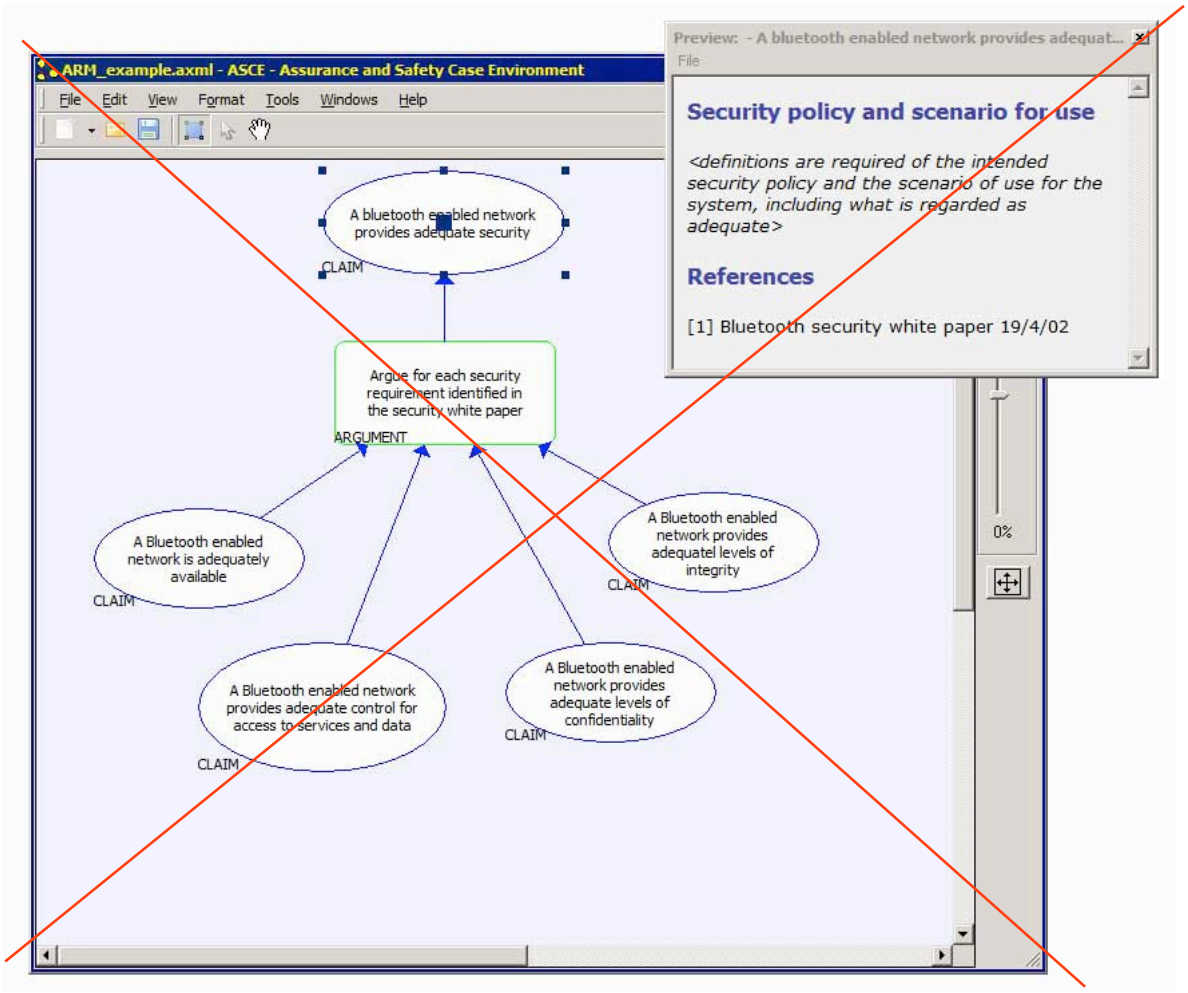
~~In CAE, contextual information can be represented either as visual nodes in a similar manner to GSN (see Figure B.3), or alternatively as rich text associated with the node (see Figure B.4).~~

~~The following table explains the relationship from the example to the modeling elements of the SACM Argumentation Metamodel.~~

~~CAE element~~	~~SACM Argumentation Metamodel counterpart~~
~~Blue clipse~~	~~Claim~~
~~Green rounded box~~	~~ArgumentReasoning~~
~~Element with no border~~	~~InformationElement~~
~~Blue arrow~~	~~AssertedInference~~
~~Green arrow~~	~~AssertedInference (unless from InformationElement, in which case AssertedContext)~~
~~Rich narrative text~~	~~InformationElement attached using AssertedContext to the current element.~~



~~**Figure B.3 - CAE of Bluetooth example - showing contextual information as visual nodes**~~



~~**Figure B.4 - CAE representation of the Bluetooth example where contextual information held as rich text (top claim is selected)**~~